(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2001016197 A**

(43) Date of publication of application: **19.01.01**

(51) Int. Cl **H04L 9/26**
G09C 1/00

(21) Application number: **11187699**

(22) Date of filing: **01.07.99**

(71) Applicant: **TOYO COMMUN EQUIP CO LTD**

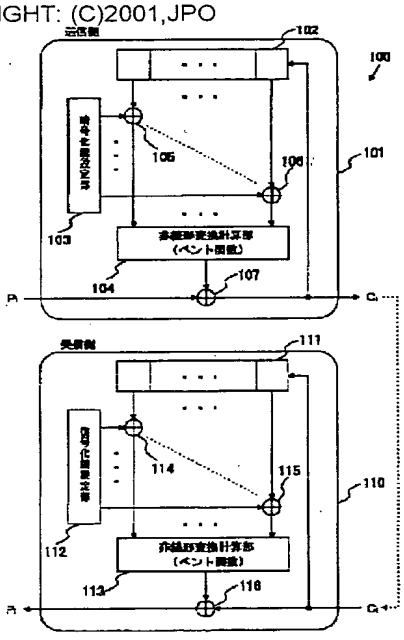
(72) Inventor: **SUGIMOTO KOICHI**

(54) SELF-SYNCHRONIZED STREAM ENCIPHERING SYSTEM AND MAC GENERATING METHOD USING THE SAME

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a self-synchronized stream enciphering system with which the mutual correlation of the sequence obtained by deciphering the cipher text, generated by a certain key, by using another key is extremely small in comparison with the sequence of plaintext and key setting is made easy.

SOLUTION: In a self-synchronized stream enciphering device 100 for inputting the plaintext bit by bit and outputting the cipher text bit by bit and having plural steps of shift registers 102, a nonlinear transformation calculating part 104 of multi-bit input and one-bit output and an encipher key setting part 103 for storing an encipher key, the nonlinear transformation calculating part 104 is provided with a bent function operating part for inputting the result of exclusively ORing the value in the shift register 102 and the setting value of the encipher key setting part 103 for each bit and outputting the operation result of a corresponding bent function and the result obtained by exclusively ORing the plaintext and the output of the non-linear conversion calculating part 104 for each bit is successively inputted to the shift register 102 and defined as a cipher text to be outputted.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2001－16197
（P2001－16197A）
(43)公開日　平成13年１月19日（2001.1.19）

(51)Int.Cl.'		識別記号	FI		テーマコード'（参考）
H04L	9/26		H04L	9/00	659　5J104
G09C	1/00	610	G09C	1/00	610D
		640			640D

審査請求　未請求　請求項の数６　ＯＬ　（全８頁）

(21)出願番号　特願平11－187699

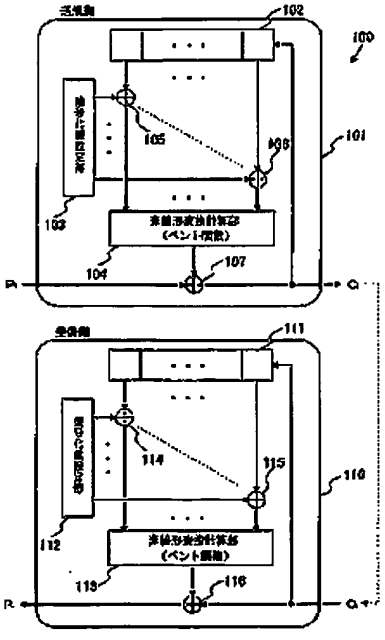
(22)出願日　平成11年７月１日（1999.7.1）

(71)出願人　000003104
東洋通信機株式会社
神奈川県高座郡寒川町小谷２丁目１番１号
(72)発明者　杉本　浩一
神奈川県高座郡寒川町小谷２丁目１番１号
東洋通信機株式会社内
(74)代理人　100098039
弁理士　遠藤　恭

Ｆターム(参考)　5j104 AA01 AA08 JA06 LA02 NA02
NA08 NA23 NA37

(54)【発明の名称】　自己同期型ストリーム暗号システム及びこれを用いたＭＡＣ生成方法

(57)【要約】
【課題】　ある鍵によって生成された暗号文の系列を異なる鍵で復号した場合の系列が、平文の系列と比較した場合、その相互相関が極めて小さくなり、かつ、鍵の設定が容易であるような自己同期型ストリーム暗号システムを提供する。
【解決手段】　本発明は、複数段のシフトレジスタ１０２と、多ビット入力１ビット出力の非線形変換計算部１０４と、暗号化鍵を格納する暗号化鍵設定部１０３とを有し、平文を１ビットずつ入力し暗号文を１ビットずつ出力する自己同期型ストリーム暗号の暗号化装置１００であって、非線形変換計算部１０４が、シフトレジスタ１０２における値と暗号化鍵設定部１０３の設定値をビット毎に排他的論理和した結果を入力とし、これに対するベント関数の演算結果を出力とするベント関数演算部を備え、前記平文と非線形変換計算部１０４の出力をビット毎に排他的論理和した結果を、シフトレジスタ１０２へ順次入力すると共に、出力される暗号文とする。



1

【特許請求の範囲】

【請求項１】　同期信号に同期して動作する複数段のシフトレジスタと．多ビット入力１ビット出力の非線形変換計算部と、ｎビットの暗号化鍵を格納する暗号化鍵設定部とを有し．前記同期信号に同期して、平文を１ビットずつ入力し．暗号文を１ビットずつ出力する自己同期型ストリーム暗号の暗号化装置であって、

前記非線形変換計算部が．前記シフトレジスタにおけるレジスタｎビットと前記暗号化鍵設定部に設定された暗号化鍵ｎビットをビット毎に排他的論理和演算した結果を少なくともその入力とし．該入力に対しベント関数による演算を行った結果を出力とするベント関数演算部を備え．

前記入力された平文と前記非線形変換計算部の出力をビット毎に排他的論理和演算した結果を．前記シフトレジスタへ順次入力すると共に．前記出力される暗号文としたことを特徴とする自己同期型ストリーム暗号の暗号化装置。

【請求項２】　同期信号に同期して動作する複数段のシフトレジスタと．多ビット入力１ビット出力の非線形変換計算部と、ｎビットの復号化鍵を格納する復号化鍵設定部とを有し．前記同期信号に同期して、暗号文を１ビットずつ入力し．復号文を１ビットずつ出力する自己同期型ストリーム暗号の復号化装置であって、

前記非線形変換計算部が．前記シフトレジスタにおけるレジスタｎビットと前記復号化鍵設定部に設定された復号化鍵ｎビットをビット毎に排他的論理和演算した結果を少なくともその入力とし．該入力に対しベント関数による演算を行った結果を出力とするベント関数演算部を備え．

前記入力された暗号文を．前記シフトレジスタへ入力すると共に、前記入力された暗号文と前記非線形変換計算部の出力をビット毎に排他的論理和演算した結果を、前記出力される復号文としたことを特徴とする自己同期型ストリーム暗号の復号化装置。

【請求項３】請求項１記載の自己同期型ストリーム暗号の暗号化装置と請求項２記載の自己同期型ストリーム暗号の復号化装置を備えて構成される自己同期型ストリーム暗号システム。

【請求項４】　請求項１記載の自己同期型ストリーム暗号の暗号化装置を用いてＮビットの平文からＳビットのメッセージ認証子を生成するＭＡＣ生成方法であって、

前記シフトレジスタに所定の初期値を設定する手順と、

前記暗号化装置にＮビットの平文を入力する手順と、

前記暗号化装置から出力されたＮビットの暗号文の末尾から連続するＳビットをメッセージ認証子として出力する手順と、を備えたことを特徴とするＭＡＣ生成方法。

【請求項５】　同期信号に同期して動作する複数段のシフトレジスタと．多ビット入力１ビット出力の非線形変換計算部と、ｎビットの暗号化鍵を格納する暗号化鍵設定部とを有し．前記同期信号に同期して、平文を１ビットずつ入力し．暗号文を１ビットずつ出力する自己同期型ストリーム暗号の暗号化方法であって、

2

前記入力された平文と前記非線形変換計算部の出力をビット毎に排他的論理和演算する手順と．

前記排他的論理和演算の結果を、前記シフトレジスタへ順次入力すると共に、前記出力される暗号文として用いる手順と、

前記シフトレジスタにおけるレジスタｎビットと前記暗号化鍵設定部に設定された暗号化鍵ｎビットをビット毎に排他的論理和演算する手順と、

前記排他的論理和演算の結果を少なくともその入力とし．該入力に対しベント関数による演算を行う手順と、

前記ベント関数による演算の結果を含んで前記非線形変換計算部の出力を生成する手順と、を備えた自己同期型ストリーム暗号の暗号化方法。

【請求項６】　同期信号に同期して動作する複数段のシフトレジスタと．多ビット入力１ビット出力の非線形変換計算部と、ｎビットの復号化鍵を格納する復号化鍵設定部とを有し．前記同期信号に同期して、暗号文を１ビットずつ入力し．復号文を１ビットずつ出力する自己同期型ストリーム暗号の復号化方法であって、

前記入力された暗号文を．前記シフトレジスタへ順次入力する手順と．

前記シフトレジスタにおけるレジスタｎビットと前記復号化鍵設定部に設定された復号化鍵ｎビットをビット毎に排他的論理和演算する手順と、

前記排他的論理和演算の結果を少なくともその入力とし．該入力に対しベント関数による演算を行う手順と、

前記ベント関数による演算の結果を含んで前記非線形変換計算部の出力を生成する手順と、

前記入力された暗号文と前記非線形変換計算部の出力をビット毎に排他的論理和演算し、その結果を、前記出力される暗号文として用いる手順と、を備えた自己同期型ストリーム暗号の復号化方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は．暗号通信装置などで利用される自己同期型ストリーム暗号システム．及び該システムを用いたＭＡＣ生成方法に関する。

【従来の技術】従来より．電話機、無線通信装置．データ通信装置のような通信システムにおいては、第三者、すなわちその通信システムの両端の通信当事者以外の者が．その通信システムで伝送される情報を知ることができないようにするために．ここで伝送される伝送情報を暗号化することが行われている。

【０００２】この暗号化の方式としては多種の方式が知られているが．高速なデータ通信に利用可能な方式としてはストリーム暗号方式がある。図４に沿って．ストリーム暗号方式の一形態である自己同期型ストリーム暗号

方式について説明する。

【０００３】図において．自己同期型ストリーム暗号システム４００は．データストリーム（平文）を暗号化する自己同期型ストリーム暗号化装置４０１（送信側）および暗号化されたストリーム（暗号文）を復号化する自己同期型ストリーム復号化装置４０５（受信側）を備える。暗号化装置４０１と復号化装置４０５は、それぞれ同じ構造のシフトレジスタ４０２、４０６、非線形変換計算部４０３．４０７を有する。

【０００４】すなわち、暗号化装置４０１は、シフトレジスタ４０２．非線形変換計算部４０３及び排他的論理和演算部４０４を備える。暗号化装置４０１では．平文P_iがビット毎に入力されると、同期信号に同期して暗号文C_iがビット毎に出力される。すなわち、平文P_iと非線形変換計算部４０３の出力は、排他的論理和演算部４０４でビット毎に排他的論理和演算され．その結果は、暗号文C_iとして出力されると共に、シフトレジスタ４０２の最右段に入力される。シフトレジスタ４０２は同期信号に同期してその記憶している内容を１ビット左シフトする。非線形変換計算部４０３はシフトレジスタ４０２の各段におけるレジスタ値を非線形変換し、結果の１ビットを出力する。

【０００５】復号化装置４０５は、シフトレジスタ４０６．非線形変換計算部４０７及び排他的論理和演算部４０８を備える。復号化装置４０５では．暗号化装置４０１から送信された暗号文C_iがビット毎に入力されると、同期信号に同期して平文P_iがビット毎に出力される。すなわち、暗号文C_iと非線形変換計算部４０７の出力は、排他的論理和演算部４０８でビット毎に排他的論理和演算され、その結果は、平文P_iとして出力される。同時に暗号文C_iは、シフトレジスタ４０６の最右段に入力される。シフトレジスタ４０６は、同期信号に同期してその記憶している内容を１ビット左シフトする。非線形変換計算部４０７はシフトレジスタ４０６の各段におけるレジスタ値を非線形変換し．結果の１ビットを出力する。

【０００６】次に、前記自己同期型ストリーム暗号システムを用いたＭＡＣ生成方法について説明する。ＭＡＣ(Message Authenticate Codes：メッセージ認証子)は、暗号化鍵に依存して、平文の特徴を抽出したデータであり．元の平文データの改ざんを検出するために利用される。ＭＡＣは暗号化鍵に依存しているので、暗号化鍵を有しない第三者によって．簡単に生成することができない。ＭＡＣを付加したデータにおいては、第三者がデータ部分を改ざんしても、ＭＡＣ部分を算出することが困難である。したがって、第三者によるデータ改ざんを検出することができる。

【０００７】暗号化方式を利用すると．簡単にＭＡＣを生成することができる。例えば、ＤＥＳ(Data Encryption Standard)などのブロック暗号方式のＣＢＣ(Cipher Block Chaining)モードを用いれば、ＭＡＣは暗号文の最終ブロックとして算出できることが知られている。

【０００８】図５は、ブロック暗号方式におけるＣＢＣモード５００を示したものである。符号５０１はブロック暗号における暗号化部であり、符号５０３、５０４はそれぞれサイズの等しい平文ブロック．暗号文ブロックを示している。符号５０５は１サイクル前の暗号文ブロックである。平文は一定のサイズのブロックに分割され．最初のブロックから順番に５０３に配置される。暗号文は暗号化部５０１から出力されたブロック５０４を順番に並べたものとなる。

【０００９】最初の暗号化では、まず．５０５に初期値が設定される。５０５に設定された初期値は５０３に入力された平文ブロックと同位置のビット毎に５０２において排他的論理和演算され．暗号化部５０１によって暗号化されて、暗号文ブロック５０４として出力される。次以降の暗号化では、５０５には前回出力された暗号文ブロックが設定される。

【００１０】上述したＣＢＣモードを用いれば．ＭＡＣは暗号文の最終ブロックとして得られる。また．図４に示した自己同期型ストリーム暗号では．非線形変換計算部４０３の出力を図５における暗号文ブロック(C_i)５０４と考え、暗号文の最終部分をＭＡＣとすることができる。

【００１１】

【発明が解決しようとする課題】しかしながら．図４に示した自己同期型ストリーム暗号システムでは．暗号化及び復号化鍵として、非線形変換計算部４０３．４０７の構造を共通にする必要があるが、その構造は複雑であるため、暗号化及び復号化鍵として扱いづらいという問題があった。

【００１２】また、鍵同士には、ある鍵によって生成された暗号文の系列を異なる鍵で復号した場合の系列と、平文の系列とを比較した場合、その相互相関が極めて小さくなるという性質が要求される。即ち、鍵同士には、復号化鍵が暗号化鍵と異なった場合．平文と全く異なった系列が生じることが必要となる。しかしながら．従来．このような性質をもった非線形変換計算部を鍵として採択する効率的な手法が存在しないといった問題もあった。

【００１３】また、従来の自己同期型ストリーム暗号システムでは、鍵の設定が容易ではないため、暗号化鍵に依存したＭＡＣの生成も困難であった。

【００１４】本発明では．前記問題点に鑑み、ある鍵によって生成された暗号文の系列を異なる鍵で復号した場合の系列が、平文の系列と比較した場合、その相互相関が極めて小さくなり、かつ．鍵の設定が容易であるような自己同期型ストリーム暗号システムを提供することを目的とする。

【００１５】また、本発明は、前記自己同期型ストリーム暗号システムを用いたＭＡＣ生成方法を提供する。

【００１６】
【課題を解決するための手段】前記目的を達成するため本発明は、同期信号に同期して動作する複数段のシフトレジスタと、多ビット入力１ビット出力の非線形変換計算部と、ｎビットの暗号化鍵を格納する暗号化鍵設定部とを有し、前記同期信号に同期して、平文を１ビットずつ入力し、暗号文を１ビットずつ出力する自己同期型ストリーム暗号の暗号化装置であって、前記非線形変換計算部が、前記シフトレジスタにおけるレジスタｎビットと前記暗号化鍵設定部に設定された暗号化鍵ｎビットをビット毎に排他的論理和演算した結果を少なくともその入力とし、該入力に対しベント関数による演算を行った結果を出力とするベント関数演算部を備え、前記入力された平文と前記非線形変換計算部の出力をビット毎に排他的論理和演算した結果を、前記シフトレジスタへ順次入力すると共に、前記出力される暗号文としたことを特徴として構成される。
【００１７】本発明はまた、同期信号に同期して動作する複数段のシフトレジスタと、多ビット入力１ビット出力の非線形変換計算部と、ｎビットの復号化鍵を格納する復号化鍵設定部とを有し、前記同期信号に同期して、暗号文を１ビットずつ入力し、復号文を１ビットずつ出力する自己同期型ストリーム暗号の復号化装置であって、前記非線形変換計算部が、前記シフトレジスタにおけるレジスタｎビットと前記復号化鍵設定部に設定された復号化鍵ｎビットをビット毎に排他的論理和演算した結果を少なくともその入力とし、該入力に対しベント関数による演算を行った結果を出力とするベント関数演算部を備え、前記入力された暗号文を、前記シフトレジスタへ入力すると共に、前記入力された暗号文と前記非線形変換計算部の出力をビット毎に排他的論理和演算した結果を、前記出力される復号文としたことを特徴として構成される。
【００１８】更に本発明は、前記自己同期型ストリーム暗号の暗号化装置と前記自己同期型ストリーム暗号の復号化装置を備えて構成される自己同期型ストリーム暗号システムである。
【００１９】また、本発明は、前記自己同期型ストリーム暗号の暗号化装置を用いてＮビットの平文からＳビットのメッセージ認証子を生成するＭＡＣ生成方法であって、前記シフトレジスタに所定の初期値を設定する手順と、前記暗号化装置にＮビットの平文を入力する手順と、前記暗号化装置から出力されたＮビットの暗号文の末尾から連続するＳビットをメッセージ認証子として出力する手順とを備えて構成される。
【００２０】本発明は、また、同期信号に同期して動作する複数段のシフトレジスタと、多ビット入力１ビット出力の非線形変換計算部と、ｎビットの暗号化鍵を格納する暗号化鍵設定部とを有し、前記同期信号に同期して、平文を１ビットずつ入力し、暗号文を１ビットずつ出力する自己同期型ストリーム暗号の暗号化方法であって、前記入力された平文と前記非線形変換計算部の出力をビット毎に排他的論理和演算する手順と、前記排他的論理和演算の結果を、前記シフトレジスタへ順次入力すると共に、前記出力される暗号文として用いる手順と、前記シフトレジスタにおけるレジスタｎビットと前記暗号化鍵設定部に設定された暗号化鍵ｎビットをビット毎に排他的論理和演算する手順と、前記排他的論理和演算の結果を少なくともその入力とし、該入力に対しベント関数による演算を行う手順と、前記ベント関数による演算の結果を含んで前記非線形変換計算部の出力を生成する手順と、を備えて構成される。
【００２１】更に本発明は、同期信号に同期して動作する複数段のシフトレジスタと、多ビット入力１ビット出力の非線形変換計算部と、ｎビットの復号化鍵を格納する復号化鍵設定部とを有し、前記同期信号に同期して、暗号文を１ビットずつ入力し、復号文を１ビットずつ出力する自己同期型ストリーム暗号の復号化方法であって、前記入力された暗号文を、前記シフトレジスタへ順次入力する手順と、前記シフトレジスタにおけるレジスタｎビットと前記復号化鍵設定部に設定された復号化鍵ｎビットをビット毎に排他的論理和演算する手順と、前記排他的論理和演算の結果を少なくともその入力とし、該入力に対しベント関数による演算を行う手順と、前記ベント関数による演算の結果を含んで前記非線形変換計算部の出力を生成する手順と、前記入力された暗号文と前記非線形変換計算部の出力をビット毎に排他的論理和演算し、その結果を、前記出力される暗号文として用いる手順と、を備えて構成される。
【００２２】
【発明の実施の形態】以下、図示した一実施形態に基いて本発明を詳細に説明する。図１は、本発明に係る自己同期型ストリーム暗号システムの一実施形態を示すブロック図である。図において、自己同期型ストリーム暗号システム１００は、データストリーム（平文）を暗号化する自己同期型ストリーム暗号化装置１０１（送信側）及び暗号化されたストリーム（暗号文）を復号する自己同期型ストリーム復号化装置１１０（受信側）を備える。これら暗号化装置１０１及び復号化装置１１０は、暗号通信を行う当事者が使用する端末に備えることができ、一方の当事者の端末に備えられた暗号化装置１０１によって暗号化された平文が、他方の当事者の端末に送信され、その復号化装置１１０によって復号化される。これらの装置は、専用のハードウェアによっても、また汎用のハードウェア及びその上で稼動されるプログラムによっても実現できることは、当業者であれば明らかであろう。
【００２３】前記暗号化装置１０１及び復号化装置１１０は、それぞれ同じ構造のシフトレジスタ１０２、１１１、及び非線形変換計算部１０４、１１３を備える。こ

れらは、端末内のハードウェア構成として共用することができる。

【００２４】暗号化装置１０１は、シフトレジスタ１０２．暗号化鍵設定部１０３．非線形変換計算部１０４及び排他的論理和演算部１０５～１０６を備える。暗号化装置１０１では．平文P_iがビット毎に入力されると、同期信号に同期して暗号文C_iがビット毎に出力される。すなわち、平文P_iと非線形変換計算部１０４の出力は、排他的論理和演算部１０７でビット毎に排他的論理和演算され．その結果は暗号文C_iとして出力されると共に、シフトレジスタ１０２の最右段に入力される。シフトレジスタ１０２は．同期信号に同期してその記憶している内容を１ビット左シフトする。排他的論理和演算部１０５～１０６は、シフトレジスタ１０２の各段におけるレジスタ値に対して．暗号化鍵設定部１０３に設定された値を．ビット毎に排他的論理和するものである。非線形変換計算部１０４は、前記排他的論理和演算部１０５～１０６の各結果を入力し、それらを非線形変換し．結果として１ビットを出力する。

【００２５】一方、復号化装置１１０は、シフトレジスタ１１１、復号化鍵設定部１１２、非線形変換計算部１１３及び排他的論理和演算部１１４～１１５を備える。復号化装置１１０では、受信した暗号文C_iがビット毎に入力されると．同期信号に同期して平文P_iがビット毎に出力される。すなわち、暗号文C_iと非線形変換計算部１１３の出力は．排他的論理和演算部１１６でビット毎に排他的論理和演算され、その結果は平文P_iとして出力される。また、復号化装置１１０では．受信した暗号文C_iは．シフトレジスタ１１１の最右段に入力される。シフトレジスタ１１１は、同期信号に同期してその記憶している内容を１ビット左シフトする。排他的論理和演算部１１４～１１５は、シフトレジスタ１１１の各段におけるレジスタ値に対して、復号化鍵設定部１１２に設定された値を、ビット毎に排他的論理和するものである。非線形変換計算部１１３は．前記排他的論理和演算部１１４～１１５の各結果を入力し、それらを非線形変換し、結果として１ビットを出力する。

＊【００２６】ここに、非線形変換計算部１０４．１１３は．ベント(Bent)関数と呼ばれる多ビット（偶数ビット）入力１ビット出力のブール関数で構成される。ベント関数の一例を符号２００として図２に示す。図において．２０４～２０７を通じて入力されたビット値は、論理積演算部２０１、２０２で演算された後に、排他的論理和演算部２０３に入力され、その結果は２０８に出力される。

【００２７】このように構成された自己同期型ストリーム暗号方式が．ある鍵によって生成された暗号文の系列を異なる鍵で復号した場合の系列が．平文の系列と比較した場合、その相互相関が極めて小さくなる。この理由を以下に示す。

【００２８】いま、図１の自己同期型ストリーム暗号システムにおける暗号化装置１０１において、時刻iにおいて入力される平文をP_i．出力される暗号文をC_i．シフトレジスタ１０２の出力を．

【００２９】

【式１】

$$s_i = (s_{i,1}, \cdots, s_{i,n}), s_{i,j} \in \{0,1\}, (1 \le j \le n)$$

で表し、ベント関数である非線形変換計算部１０４の入力を．

【００３０】

【式２】

$$x_i = (x_{i,1}, \cdots, x_{i,n}), x_{i,j} \in \{0,1\}, (1 \le j \le n)$$

出力を、

【００３１】

【式３】

$$z_i = f(x_i) \in \{0,1\}$$

で表したとする。但し、ｎは偶数である。このとき、暗号化鍵設定部１０３に設定される暗号化鍵を、

【００３２】

【式４】

$$\mathbf{k} = (k_1, \cdots, k_n), k_j \in \{0,1\}, (1 \le j \le n)$$

とすれば、

【００３３】

【式５】

$$x_i = s_i \oplus \mathbf{k}$$

である。ただし．

【００３４】

【式６】

$$s_i \oplus \mathbf{k} = (s_{i,1} \oplus k_1, \cdots, s_{i,n} \oplus k_n)$$

であり、

【外１】

$\oplus$

は排他的論理和演算を示す。また、暗号文C_iは．

【００３５】

【式７】

$$c_i = p_i \oplus f(x_i) = p_i \oplus z_i$$

によって計算される。これら暗号文がシフトレジスタ１０２に入力されるため、シフトレジスタ１０２においては．その内部状態は、

【００３６】

【式８】

$$s_i = (c_{i-1}, \cdots, c_{i-n})$$

と表すことができる。いま．平文P_i同士が統計的にランダムであり、時間的にも相関が全くないと仮定すると、式７より、暗号文C_i同士も統計的にランダムとなり、また．時間的にも相関がないことになる。これは．いかなる情報源からの系列であってもランダムな情報源からの系列と非他的論理和演算を施せばランダムな系列となるという享実から容易に理解できる。

【００３７】復号化装置１１０において、時刻iにおけるシフトレジスタ１１１の出力を、暗号化装置１０１と同様に、式１．ベント関数である非線形変換計算部１１３の入力を式２．出力を式３で表したとする。また、復号化鍵設定部１１２に設定される復号化鍵は、暗号化鍵と同じ値、すなわち式４とする。このとき、平文P_iは次のように復号化される。

【００３８】

【式９】

$$p_i = c_i \oplus z_i = c_i \oplus f(x_i)$$

＊式９に、式５．式６及び式８を適用すれば、次式を得る。

【００３９】

【式１０】

$$p_i = c_i \oplus f(c_{i-1} \oplus k_1, \cdots, c_{i-n} \oplus k_n)$$

いま．復号化鍵設定部１１２に、暗号化に用いた鍵と異なる鍵、

【００４０】

【式１１】

$$\mathbf{k}' = (k'_1, \cdots, k'_n), k'_j \in \{0,1\}, (1 \le j \le n)$$

を設定したとする。このとき、復号化装置１１０の出力P'_iは次式のように表される。

【００４１】

【式１２】

$$p'_i = c_i \oplus f(c_{i-1} \oplus k'_1, \cdots, c_{i-n} \oplus k'_n)$$

ここにP_iとP'_iの相互相関は、

【００４２】

＊【式１３】

$$p_i \oplus p'_i = f(c_{i-1} \oplus k_1, \cdots, c_{i-n} \oplus k_n) \oplus f(c_{i-1} \oplus k'_1, \cdots, c_{i-n} \oplus k'_n)$$

における１、０の出現頻度によって観測することができる。特に、１．０の出現頻度が等しければ相互相関はないことになる。式１３は．

【００４３】

【式１４】

$$(c_{i-1} \oplus k_1, \cdots, c_{i-n} \oplus k_n) = (u_{i,1}, \cdots, u_{i,n}) = u_i$$

※とおくことにより、次式となる。

【００４４】

【式１５】

$$p_i \oplus p'_i = f(u_i) \oplus f(u_i \oplus \mathrm{b})$$

ただし、

【００４５】

※【式１６】

$$b = (b_1, \cdots, b_n) = (k_1 \oplus k'_1, \cdots, k_n \oplus k'_n)$$

である。ここに．fはベント関数である。ベント関数においては、以下の性質が知られている。すなわち．ベント関数fにおいては．

【００４６】

【式１７】

$$\sum_{x \in \{0,1\}^n} f(x) \oplus f(x \oplus a) = 2^{n-1}$$

なる性質がある。但し、$a \in \{0,1\}^n$．$a \neq \{0,0,\ldots 0\}$である。この享実は、Seongtack Chee. Sangjin Lee, kwangjo Kim著の論文、"Semi-bent functions, Advances in Cryptology ASIACRYPT'94,LNCS 914, Springer-Verlag, pp.107-118,1995"等に記されている。

【００４７】前記の享実を踏まえた上で、前に述べたように．平文P_i同士が統計的にランダムであり、時間的にも相関が全くないと仮定すると、$C_{i-1},\ldots,C_{i-n}$は統計的にランダムであり、時間的にも相関が全くないことになるから、式１５におけるU_iもランダムとみなせることになる。したがって、式１５に式１７の結果を適用することにより、

【００４８】

【式１８】

$$\sum_{i=1}^{2^n} p_i \oplus p'_i = \sum_{k=1}^{2^n} f(u_i) \oplus f(u_i \oplus \mathrm{b}) = 2^{n-1}$$

が得られる。これは、ある鍵によって生成された暗号文の系列を異なる鍵で復号した場合の系列が、前記暗号文の生成に用いた平文の系列と比較した場合、その相互相関が極めて小さくなることを示す。

【００４９】次に、図３は．前記自己同期型ストリーム暗号システムにより生成されるＭＡＣを示したものである。図において符号３００は、前記自己同期型ストリーム暗号システム１００によって、平文Ｎビットから生成されたＮビットの暗号文である。該暗号文３００において．その末尾から連続するＳビット部分３０１をＭＡＣとして用いることができる。

【００５０】以上、本発明の一実施形態を図面に沿って説明した。しかしながら本発明は前記実施形態に示した享項に限定されず、特許請求の範囲の記載に基いてその変更．改良等が可能であることは明らかである。例えば．前記非線形変換計算部は、鍵設定部の値がそのベント関数へ入力される限り．以下のように構成しても良い。

（１）非線形変換計算部のベント関数には、シフトレジスタと鍵設定部の排他的論理和の結果以外の入力、例えば、シフトレジスタの他のビット値を入力しても良い。

（２）非線形変換計算部の出力は、ベント関数による演算結果と他の演算結果を排他的論理和したものとしても良い。

【００５１】

【発明の効果】以上の如く本発明によれば、ある鍵によって生成された暗号文の系列を異なる鍵で復号した場合の系列が、平文の系列と比較した場合、その相互相関が極めて小さくなり、かつ、鍵の設定が容易であるような自己同期型ストリーム暗号システムを提供することが可能になる。

【図面の簡単な説明】

【図１】本発明に係る自己同期型ストリーム暗号システムの一実施形態を示すブロック図である。

【図２】ベント関数の一例を示すブロック図である。

【図３】本発明に係る自己同期型ストリーム暗号システムにより生成されるＭＡＣを示した図である。

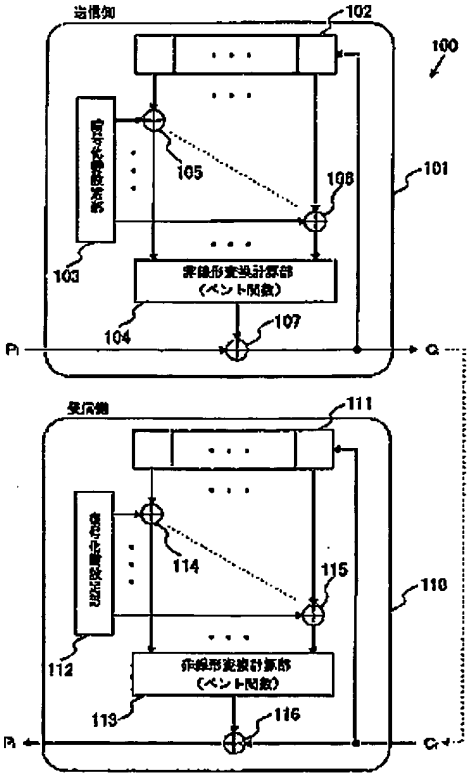
【図４】従来の自己同期型ストリーム暗号システムのブ＊ロック図である。

＊【図５】ブロック暗号方式におけるＣＢＣモードを示す図である。

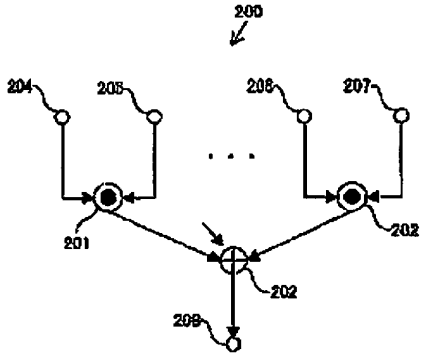
【符号の説明】

１００　自己同期型ストリーム暗号システム
１０１　自己同期型ストリーム暗号化装置
１０２　シフトレジスタ
１０３　暗号化鍵設定部
１０４　非線形変換計算部
１０５～１０６　排他的論理和演算部
１０７　排他的論理和演算部
１１０　自己同期型ストリーム復号化装置
１１１　シフトレジスタ
１１２　復号化鍵設定部
１１３　非線形変換計算部
１１４～１１５　排他的論理和演算部
１１６　排他的論理和演算部
２０１、２０２　論理積演算部
２０３　排他的論理和演算部

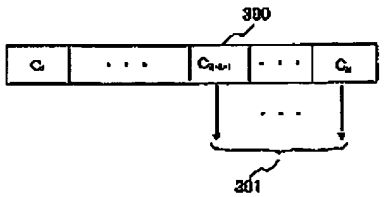
【図１】



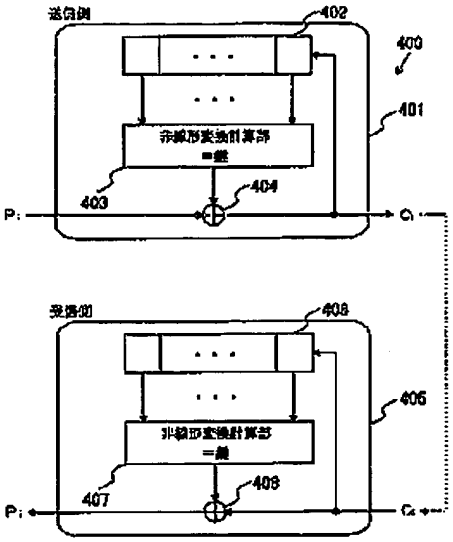
【図２】



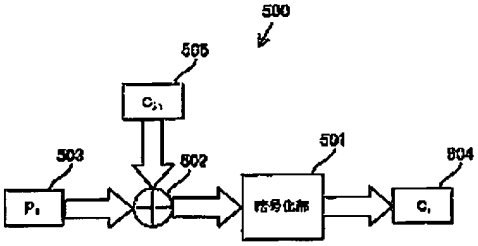
【図３】



【図４】


送信側
402
400
401
非線形変換計算部
403
404
P_i
C_i
受信側
408
406
非線形変換計算部
407
408
P_i
C_i

【図５】


500
505
C_{i-1}
503
502
501
504
P_i
信号伝播
C_i